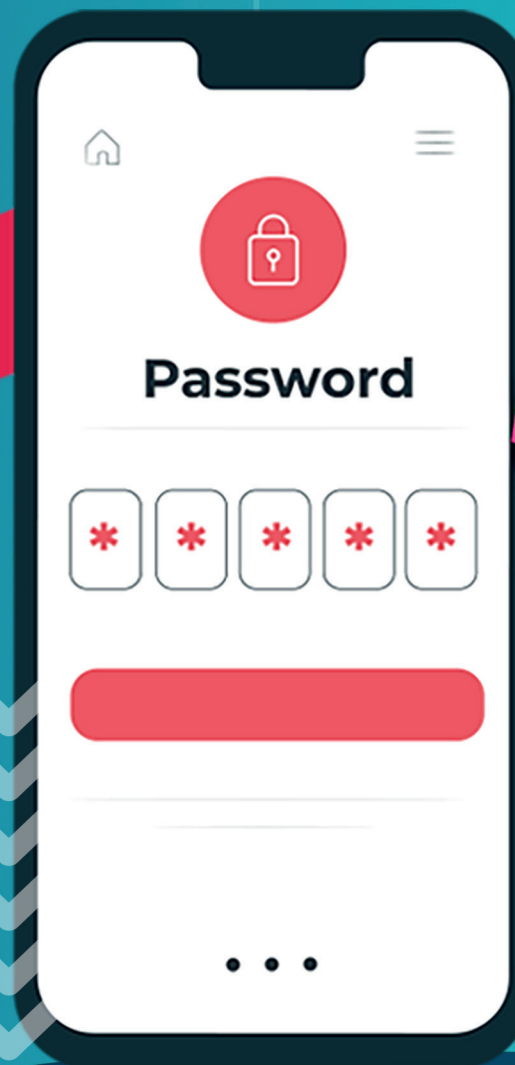


GESTIÓN DE CONTRASEÑAS SEGURAS

*Protege tu identidad digital
con hábitos seguros*

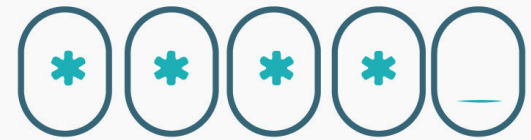


1. UTILIZA CONTRASEÑAS FUERTES Y ÚNICAS

“Tu contraseña es como tu cepillo de dientes: debe ser personal, segura y cambiarse con frecuencia.”



Contraseña



Esta contraseña es segura

¿Por qué es importante?

- Una contraseña robusta previene accesos no autorizados a tus cuentas.
- Combinaciones débiles como "123456" pueden ser adivinadas en segundos.
- Si usas la misma contraseña en varias cuentas, una sola filtración compromete todas tus credenciales.
- Usa al menos 12 caracteres, combinando mayúsculas, minúsculas, números y símbolos.

Recomendaciones:

- Crea contraseñas seguras usando técnicas como:

Tomar la primera letra de cada palabra de una frase personal.

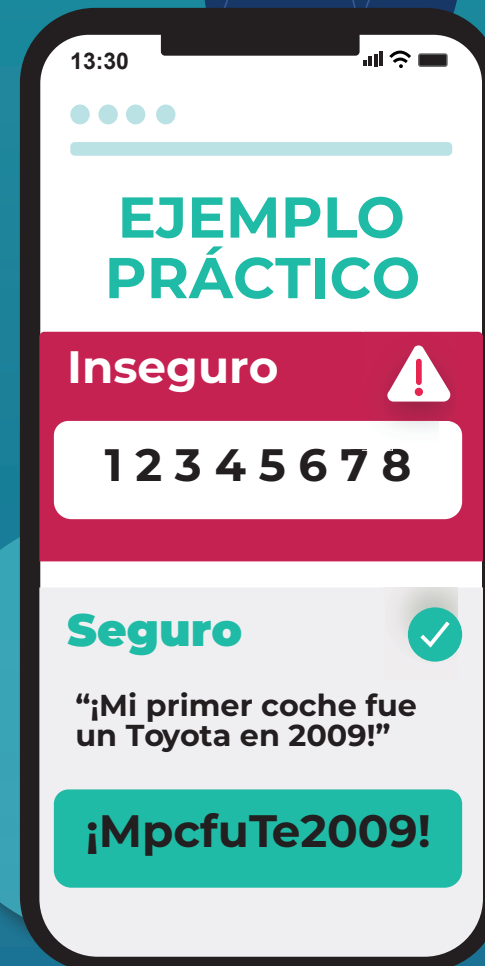
Combinar palabras con números y símbolos.

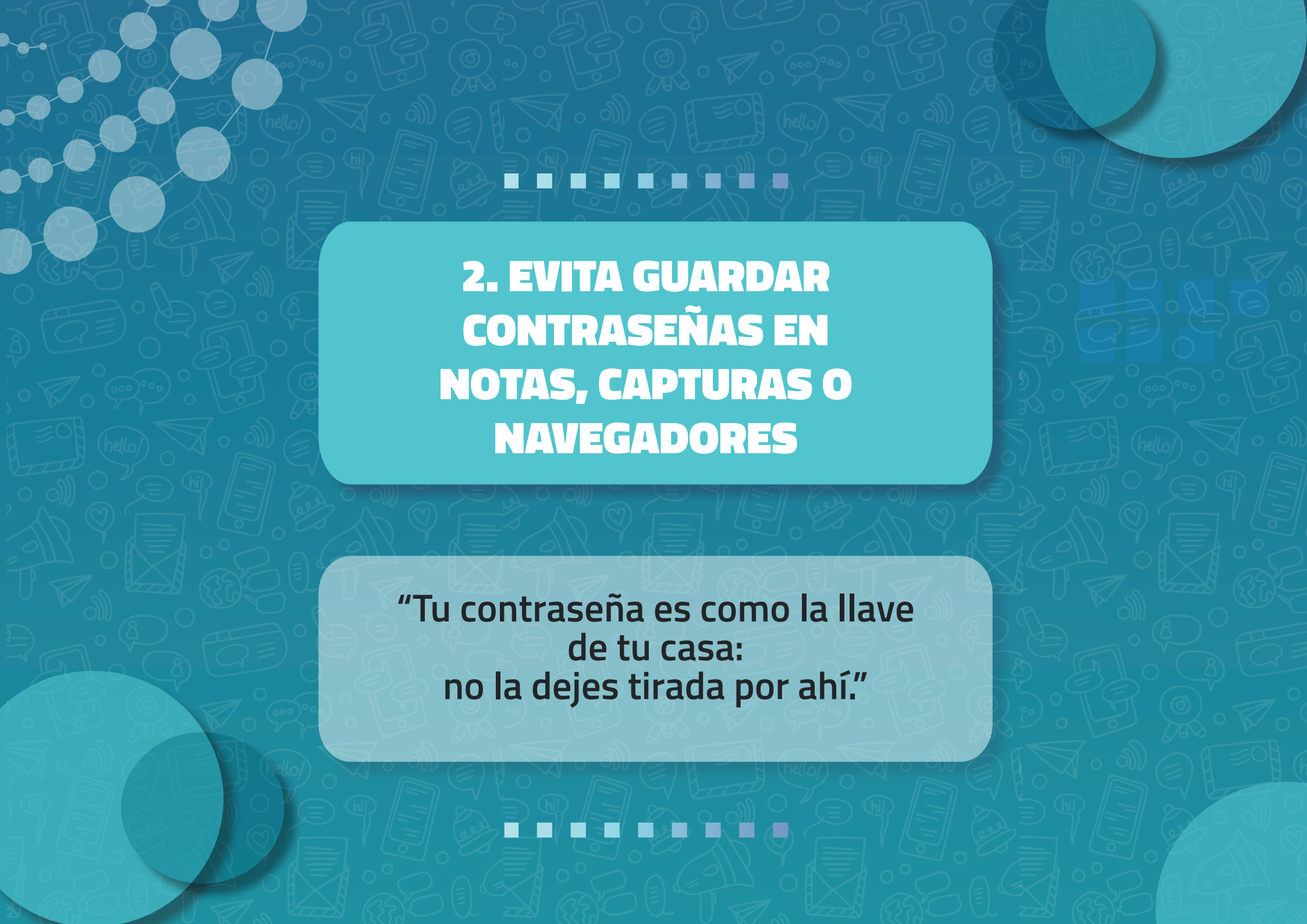
Usar patrones memorizables en el teclado.

Evita nombres, fechas o palabras comunes.

Usa una contraseña distinta para cada cuenta.

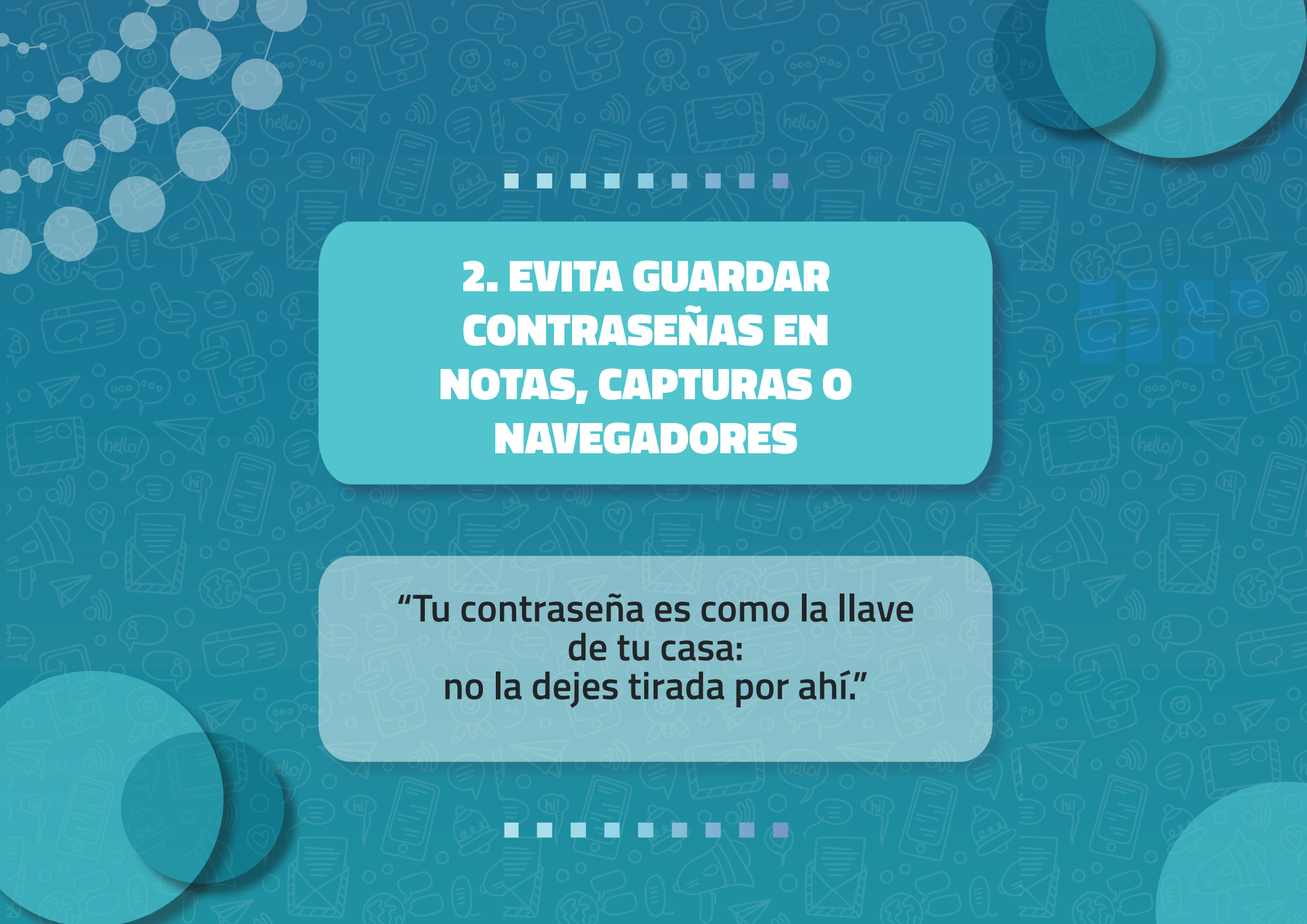
- Cámbialas periódicamente o utiliza un gestor de contraseñas confiable





2. EVITA GUARDAR CONTRASEÑAS EN NOTAS, CAPTURAS O NAVEGADORES

**“Tu contraseña es como la llave
de tu casa:
no la dejes tirada por ahí.”**



¿Por qué es importante?

- Si alguien accede a tu dispositivo o archivos, puede encontrar tus contraseñas fácilmente.
- Malware o virus pueden extraer contraseñas almacenadas en navegadores o archivos sin protección.

Recomendaciones:

- No guardes contraseñas en notas de papel ni archivos digitales como mensajes, capturas o imágenes.
- No uses el navegador web para almacenarlas.
- Utiliza siempre un gestor de contraseñas seguro.



3. NO COMPARTAS TUS CONTRASEÑAS

“Un secreto compartido ya no es secreto. Una contraseña compartida ya no es segura.”



¿Por qué es importante?

- **Compartir contraseñas expone tus datos a usos no autorizados.**
- **No puedes controlar cómo, cuándo ni con qué fin se usará.**
- **En manos equivocadas, tu información puede ser utilizada para fraude, chantaje o robo de identidad.**

Recomendaciones:

- **Nunca digas tu contraseña en voz alta.** Parece obvio, pero en una videollamada o en un lugar público cualquiera puede estar escuchando.
- **Si alguna vez la compartiste, cámbiala de inmediato.**
- **Incluso con personas de confianza, la prevención es la mejor opción.**





4. REvisa si tus contraseñas han sido filtradas



**"Si tu contraseña se filtró, cámbiala
antes de que un ciberdelincuente
lo haga por ti."**



¿Por qué es importante?

- Millones de contraseñas se filtran en bases de datos robadas.
- Cuanto más tiempo pase, mayor es el riesgo de que se usen en ataques automatizados.
- Muchas personas no se enteran hasta que ya es demasiado tarde.
- Una contraseña comprometida puede ser usada para suplantación, fraude o accesos no autorizados.

Recomendaciones:

- Consulta en [Have I Been Pwned](#) si tus contraseñas han sido comprometidas.
- Si lo han sido, cámbialas inmediatamente.
- Sustitúyelas por contraseñas fuertes y únicas.





5. USA GESTORES DE CONTRASEÑAS

“No memorices 100 contraseñas: recuerda una sola contraseña maestra y guarda el resto en un gestor.”

¿Por qué es importante?

- Los gestores permiten crear, guardar y autocompletar contraseñas de forma segura.
- Facilitan el uso de contraseñas únicas sin depender de la memoria.
- Protegen tus credenciales incluso si cambias de dispositivo.
- Las contraseñas almacenadas se protegen mediante cifrado.



Recomendaciones:

- Usa gestores confiables como Bitwarden, 1Password, KeePass o similares.
- Mantén el software del gestor actualizado.
- Protege el acceso con una contraseña maestra robusta y autenticación en dos pasos (2FA).

Ejemplo práctico:

▼ Carlos anotaba sus contraseñas en una libreta que perdió junto con su mochila. No pudo recuperar varias cuentas. Desde entonces, usa un gestor de contraseñas con clave maestra y verificación en dos pasos. Solo necesita recordar una... y duerme tranquilo.



6. PROMUEVE ESTOS CONSEJOS EN TU ENTORNO

“Haz que tu familia, amigos
y compañeros también
mantengan sus contraseñas
seguras.”



¿Por qué es importante?

- Todos somos parte del eslabón de seguridad. Si alguien cercano es vulnerable, tú también podrías estar en riesgo.
- Promover estas prácticas multiplica el efecto protector.
- Usa gestores confiables como Bitwarden, 1Password, KeePass o similares.

Recomendaciones:

- Comparte este dossier con tu familia, amistades y colegas.
- Capacita a tu entorno sobre la gestión segura de contraseñas.
- Fomenta una cultura de responsabilidad digital compartida.



CONCLUSIÓN

*La seguridad comienza con una contraseña...
pero no termina ahí.*

TUS PRIMEROS PASOS HOY:



Cambia tu contraseña más débil.



Revisa si ha sido filtrada en internet.



Instala y configura un gestor de contraseñas confiable.



Activa la verificación en dos pasos (2FA) en todas tus cuentas.



AGETIC
Digitalizando Bolivia